IDENTITY THEFT TOOLKIT

How to Recover From and Avoid Identity Theft

John Lenardon

Self-Counsel Press
(a division of)
International Self-Counsel Press Ltd.
USA Canada

CONTENTS

1

WHAT IS IDENTITY THEFT?

Identity theft is the fastest-growing nonviolent crime in North America today. When someone steals personal information from you such as your driver's license number, social security number, or social insurance number, or other identifying information to use for illegal purposes, you have become a victim of identity theft.

The thief could use your personal information to apply for credit cards in your name or open a checking account and write bad checks in your name. Your credit rating and your reputation could be severely damaged.

Victims of identity theft often suffer substantial economic and emotional harm. A victim will spend significant amounts of time fighting problems such as bounced checks, loan denials, credit card application rejections, and debt-collection harassment. Many victims also report feeling personally violated.

Thieves have stolen identities of teens and changed the birth dates. In some cases, teenagers applying for college loans have been told their credit rating was destroyed years ago.

There have even been cases in which an identity thief used the victim's name when caught during a criminal act. Some ID

theft victims face criminal investigation, arrest, or conviction because of the thieves' activities. For example, one victim was the subject of an arrest warrant based on speeding tickets issued to an ID thief. Some victims have also been denied employment or lost their jobs as a result of their identities having been stolen and used in illegal activities.

On April 13, 2005, Chris Swecker, the assistant director of the Criminal Investigative Division, Federal Bureau of Investigation, appeared before the Senate Judiciary Committee.

He stated, "Identity theft has emerged as one of the dominant white-collar crime problems of the 21st century. Estimates vary regarding the true impact of the problem, but agreement exists that it is pervasive and growing. In addition to the significant harm caused to the monetary victims of the frauds, often providers of financial, governmental or other services, or the individual victim of the identity theft may experience a severe loss in their ability to utilize their credit and their financial identity."

A report to the Attorney General of the United States and the Minister of Public Safety and Emergency Preparedness Canada indicated that identity theft was growing rapidly, due in part to the Internet and modern technology.

During a one-year period, total losses to individuals and businesses related to identity theft in the United States were estimated at approximately US $53 billion. In Canada, the losses for the same period were estimated at approximately CDN $2.5 billion.

A US Federal Trade Commission identity theft survey found that victims had spent a total of 300 million hours in the preceding year to resolve problems created by the theft of their identities.

All the current data show that identity theft will continue to grow substantially over the next decade and pose a threat to tens of millions of people and businesses in Canada and the United States.

WHAT DOES PERSONAL INFORMATION INCLUDE?

Any information that describes or identifies you is considered personal information.

This information could exist in any number of forms. For example, you may have had an ID-badge picture taken at work, paid a parking ticket, applied for credit cards or a mortgage, or bought a car. In each case, you have released some personal information.

Some of this information is harmless and is useless to identity thieves. However, some of it is dangerous and needs to be controlled and protected.

Some examples of personal information that you should protect are your —

- birth date,
- city of birth,
- driver's license number,
- passport number,
- home address,
- social security number or social insurance number,
- phone numbers,
- e-mail addresses, and
- family members' names and birth dates.

More than ever before, companies and governments are asking for your personal data. Every time you apply for credit, get a new job, make travel arrangements, or even make a purchase at a store, someone is demanding your information. Unfortunately, every time you release this information, the risk that it will be stolen increases. You could spend months or years trying to clear your name.

No computer system is guaranteed secure. Some of the largest companies in the world have had client records stolen. So

have government agencies and employers. No organization can fully protect your data from the constant attacks they face.

Identity theft has become big business for criminals. The amount of money involved is enormous and increases each year. As the criminal profits grow, so will the attacks.

It's up to you to learn how to protect your personal information and do everything you can to ensure it never is used to steal your identity.

IDENTITY THEFT AND TECHNOLOGY

Today, our personal data is more vulnerable than ever. It isn't something you can replace. It can't be insured nor can it be locked up in a safe. Once it is stolen, it is "out there" forever, and you can never be certain it will be safe again.

We live in an age of technology in which everything seems possible. We can store millions of records on a device that can fit in your pocket, and a single laptop computer can store hundreds of thousands of client records. In addition, almost every computer in the world is connected to public communication lines.

Unfortunately, there is one very weak link in all this technology. We can't completely protect the data. The tighter we make security, the less efficient the systems become. We could go to the extreme and lock up the data so that no one can access it, but such a step is neither economical nor sensible. Therefore, we must always compromise. In most cases, the need for easy access to the data outweighs the danger of it being stolen.

Some organizations demand access to our personal information, and others ask for it, but the result for us is the same. Whenever we give them any of our personal information, it becomes easier to steal.

Personal information has been stolen from all kinds of organizations including government departments and credit reporting agencies. The very people who publish long, detailed policies on how they will protect our data are incapable of doing so, and it is unlikely this situation will change.

HOW DO IDENTITY THIEVES STEAL INFORMATION?

Although technology can make it difficult for you to protect your information, it is only part of the problem. Identity thieves often use surprisingly low-tech methods to obtain your personal information. For instance, they steal your wallet or purse, or they steal mail from your mailbox.

Or a thief will break into your car or house. In many of these cases, the real reason behind the break-in is not to steal your personal property; it is to steal your personal information.

What follows here is a list of some of the most common methods used by ID thieves to steal your information. Just a quick glance is enough for you to see the scope of the problem:

- "Skimming" your credit cards at restaurants or stores
- Shoulder surfing your PIN at an ATM
- Picking up a bank deposit slip you used as scrap paper and threw away
- Hacking into your computer at home or at work
- Stealing your laptop or personal computer
- Sending you fake e-mails that trick you into releasing personal information
- Going through your garbage at home or at work
- Stealing your information from companies where you have accounts
- Stealing information while staying as a guest in your house

WHAT HAPPENS TO YOUR PERSONAL INFORMATION?

Personal information is a highly prized and very versatile commodity. Once a thief has your personal information, he or she can put it to all kinds of illegal uses — all of which can be extremely costly to you. Consider the following favorite activities of ID thieves:

- They get checks or debit cards made in your name and use them to empty your bank accounts.
- They take out loans or second mortgages in your name.
- They open new credit card accounts in your name. (Sometimes they use a mailing address other than yours, so it may take you weeks or months to realize that you have a problem.)
- They open a bank account in your name and write bad checks on the account.
- They establish Internet services in your name.
- They establish telephone or utility services in your name.
- They obtain automobile loans in your name.
- They use your stolen identity if they are arrested for a crime. When they do not appear for the court date, you could be arrested.
- They go on spending sprees using your credit and debit cards to buy "big ticket" items, such as computers, that they can easily sell.
- They file for bankruptcy under your name to avoid paying debts they have incurred using your identity.
- They use your identity in a marriage ceremony and use the marriage license to get immigration status in the country.
- They open accounts at a brokerage house and leave you liable for any losses.
- They use your social security number or social insurance number to get a job, leaving you liable for taxes due on that income.
- They could use your social security number or social insurance number to file a tax return and receive your refund.

No matter which one — or combination — of these crimes is committed against you, you will be left with the problem of clearing your name and rebuilding your credit rating, and you

could also be left with a large debt load or a criminal record. Restoring your credit rating or removing incorrect criminal records can take months of letter writing, phone calls, and personal expense. Unfortunately, years later, the data could resurface, and you could become a victim again.

On November 30, 2005, the Internet Crime Complaint Center (IC3) issued the following warning:

ATTENTION — E-MAIL DISGUISED AS THE INTERNAL REVENUE SERVICE (IRS) PHISHING FOR PERSONAL INFORMATION

The FBI has become aware of a spam e-mail claiming the recipient is eligible to receive a tax refund for $571.94. The e-mail purports to be from tax-returns@irs.gov with the subject line of "IRS Tax Refund." A link is provided in the e-mail to access a form required to be completed in order to receive the refund. The link appears to connect to the true IRS website. However, the recipient is redirected to http://www.porterfam.org/2005/, where personal data, including credit card information, is captured.

THIS E-MAIL IS A HOAX. DO NOT FOLLOW THE PROVIDED LINK.

DETECTING IDENTITY THEFT

How would you know if your identity was stolen? In some cases, you may not discover it for months. However, there are early warning signs you should watch for:

- Your credit card statement or bank statement does not arrive in the mail as expected. (An identity thief may have submitted a change of address notice to your financial agency so you do not detect the charges he or she placed on your cards.)

- Your bank or credit card statement contains transactions that you did not authorize. (If this happens to you, check with your financial institution or lender immediately. Sometimes a thief will make a purchase for a few dollars to test your card. If the transaction is approved, he or she will immediately go on a large spending spree.)
- Your mail stops arriving. (The ID thief may have placed a change of address at the post office.)
- You receive credit card bills for unknown accounts. (The thief may have already applied for credit in your name.)
- You get a call from a collection agency for a debt you did not incur.
- You apply for credit from a lender and are unexpectedly denied it.
- You order your credit report and find accounts or debts listed that do not belong to you.
- A lender contacts you to discuss a credit application you did not submit.
- You receive a call or letter stating that you have been approved for or denied a loan by unknown creditors.
- You receive unknown utility or telephone statements in your name and address.

These are all indications of potential identity theft. If you notice any of them, you must immediately investigate the situation and take steps to correct it. By responding quickly, you stand a chance of controlling the damage.

HOW SAFE IS YOUR IDENTITY?

Protecting your personal information takes effort on your part. To understand how great your personal risk is, try taking the Identity Risk Test in Checklist 1. Each statement represents a possible risk factor. Read each statement carefully, and if you agree with it, check the box beside it. When you are finished the test, count up all the check marks and compare that number to the results shown in Table 1.

Checklist 1
Your Identity Risk Test

Question	Check
I don't order an annual credit report to check for fraud or mistakes.	
I carry my SSN or SIN card and other unnecessary cards in my wallet or purse.	
I don't crosscut shred banking and credit information when I throw it in the trash.	
I don't crosscut shred preapproved credit offers or convenience checks (from credit card companies) when I receive them.	
I don't believe people would root around in my trash looking for credit or financial information.	
I don't conceal personal information in my house from all relatives and visitors.	
My mail is delivered to an unsecured mailbox.	
My outgoing mail is put in an unsecured mailbox.	
I don't regularly update my software for security.	
I provide personal information whenever asked, without asking how it will be used or if it is necessary for me to divulge it.	
I don't check for people who might be listening when I give out information.	
My SSN or SIN is publicly displayed or used at work or school (for example, on timecards, receipts, or badges, etc.).	
When I enter my PIN, I don't cover it with my hand.	
I allow credit cards or other identification cards to remain in public sight when making purchases.	
I allow my credit cards to leave my sight when making a purchase.	
I might click on an e-mail link if the e-mail asks me to update my data at my bank or my favorite shopping sites.	
I have a listed phone number.	
I sometimes respond to Internet surveys or telephone solicitors.	
I keep my car registration papers in the glove box.	
I keep personal papers in my car.	
I don't have strong Internet protection software or hardware on my computer.	
I don't teach my children about computer security.	
I don't teach my children to keep personal information private when talking to strangers or friends.	
Total number of check marks	

Table 1
Identity Risk Test Results

Over 5 check marks	You are at high risk of ID theft.
1 to 5 check marks	You understand identity theft, but still need to do more to protect yourself and your family.
0 check marks	Congratulations. Keep up the good work!

HOW THIS BOOK CAN HELP YOU

By now, you've probably realized that you must begin to think about and treat your personal information in an entirely different way than you have done until now. You have to protect it like you would a child. You have to keep it safe and establish control over who has access to it and how it can be used.

No longer will you gladly answer questions when credit grantors ask or automatically give personal data to retailers simply because they say they need to know. Now you must ask them why they need to know. You will only release what is necessary — and no more. And you will demand they protect it from thieves, both inside and outside their companies, and make them explain their security precautions to your satisfaction.

This book will look at the ways you can protect your information so you never become a victim of identity theft. And if it is too late for you and your identity has already been stolen, this book will show you how to restore your reputation and your credit rating. It includes all the necessary contact numbers and forms to help you deal with the problems you will face.

Keep this book as a reference if you are not a victim and as a repair manual if you are.

In one notorious case of identity theft, the criminal, a convicted felon, not only incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but also called his victim to taunt him, saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time. The thief then filed for bankruptcy, also in the victim's name.

In this case, the victim reported he spent more than four years restoring his credit. It cost him more than $15,000.